

# [UNIX] Online Store Kit SQL Injection Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0045.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 02/17/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 17 Feb 2004 18:39:36 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Online Store Kit SQL Injection Vulnerability

---

## SUMMARY

<<http://www.ecommerce.com/>> Online Store Kit "package includes all of the features that are essential for a usable shopping cart with uninterrupted functioning. If your e-commerce needs don't go far, but the products/services you offer have the demand, this package is for you". Due to improper filtering of user provided data, a remote attacker can insert malicious characters into the SQL statement used by the product.

## DETAILS

Vulnerable Systems:

\* Online Store Kit version 3.0

Examples:

SQL Injection:

By submitting the following URL, a user can insert into the existing SQL statement his own SQL code:

[http://vulnerablesite/more.php?id='\[SQL injection here\]&](http://vulnerablesite/more.php?id='[SQL injection here]&)

XSS Attack:

As the server returns the data sent by the user whenever an error occurs, cross site scripting is also possible:

Securiteam: [UNIX] Online Store Kit SQL Injection Vulnerability

[http://vulnerablesite/more.php?id=%3Cscript%3Ealert\(document.domain\);%3C/script%3E&](http://vulnerablesite/more.php?id=%3Cscript%3Ealert(document.domain);%3C/script%3E&)

ADDITIONAL INFORMATION

The information has been provided by <mailto:iamroot@systemsecure.org>  
David Sopas Ferreira.

The original article can be found at:

<<http://www.systemsecure.org/advisories/ssadvisory16022004.php>>  
<http://www.systemsecure.org/advisories/ssadvisory16022004.php>.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.